Biometrics Overview

Introduction

"Biometrics" is a general term used alternatively to describe a characteristic or a process.

As a characteristic:

1. A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.

As a process:

2. Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Biometric systems have been researched and tested for a few decades, but have only recently entered into the public consciousness because of high profile applications, usage in entertainment media (though often not realistically) and increased usage by the public in day-to-day activities. Example deployments within the United States Government include the FBI's Integrated Automated Fingerprint Identification System (IAFIS), the US-VISIT program, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program. Many companies are also implementing biometric technologies to secure areas, maintain time records, and enhance user convenience. For example, for many years Disney World has employed biometric devices for season ticket holders to expedite and simplify the process of entering its parks, while ensuring that the ticket is used only by the individual to whom it was issued.

A typical biometric system is comprised of five integrated components: A **sensor** is used to collect the data and convert the information to a digital format. **Signal processing algorithms** perform quality control activities and develop the biometric template. A **data storage** component keeps information that new biometric templates will be compared to. A **matching algorithm** compares the new biometric template to one or more templates kept in data storage. Finally, a **decision process** (either automated or human-assisted) uses the results from the matching component to make a system-level decision.

Biometric Modalities

Commonly implemented or studied biometric modalities include fingerprint, face, iris, voice, signature and hand geometry. Many other modalities are in various stages of development and assessment. There is not one biometric modality that is best for all implementations. Many factors must be taken into account when implementing a biometric device including location, security risks, task (identification or verification), expected number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity.

Fingerprint Recognition

Manual comparison of fingerprints for recognition has been in use for many years, and has become an automated biometric identification technique over the past two decades. Fingerprints have an uneven surface of ridges and valleys that form a unique pattern for each individual. For most applications, the primary interest is in the ridge patterns on the top joint of the finger.

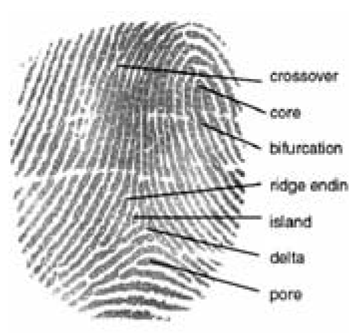

Figure 1: Fingerprint Recognition[1]

An important distinction to make is the difference between the FBI's IAFIS[2] system and the commercial fingerprint systems used for verification purposes. The FBI IAFIS system was developed to compare submitted fingerprint information against a database of several million fingerprints to determine if the individual has previously submitted fingerprints, and thus has a potential criminal history. IAFIS systems require information from all ten fingers, either ink-based or electronic, and preferably rolled impressions. Submitted fingerprints are compared against the fingerprints on file and are verified by 0, 1, or 2 fingerprint examiners. The process usually takes about two hours.

Commercial fingerprint systems that are used for verification purposes usually require only one finger to compare the fingerprint to the one on file to confirm the individual's claimed identity. This process is completely automated and usually takes less than a second. The two types of systems are not connected at all.

Face Recognition

Humans recognize familiar faces with considerable ease, but they are not good at recognizing unfamiliar individuals. Since the 1960s, machine vision researchers have been developing automated methods for recognizing individuals via their facial characteristics. Despite the volumes of research, there are no agreed-upon methods for automated face recognition as there are for fingerprints. Multiple approaches have existed for several years using low resolution 2D images. Recent work in high resolution 2D and 3D shows the potential to greatly improve face recognition accuracy.

Iris Recognition

The iris is the colored portion of an individual's eye. The concept of using the iris for recognition purposes dates back to 1936.[3] The next major advancement appeared in the late 1980s, with a patent being issued in 1994 for the algorithms that can perform iris recognition automatically. To obtain a good image of the iris, identification systems typically illuminate the iris with near-infrared light, which can be observed by most cameras yet is not detectable by, nor can it cause injury to, humans. A common misconception is that iris recognition shines a laser on the eye to "scan" it. This is incorrect untrue. Iris recognition simply takes an illuminated picture of the iris without causing any discomfort to the individual.

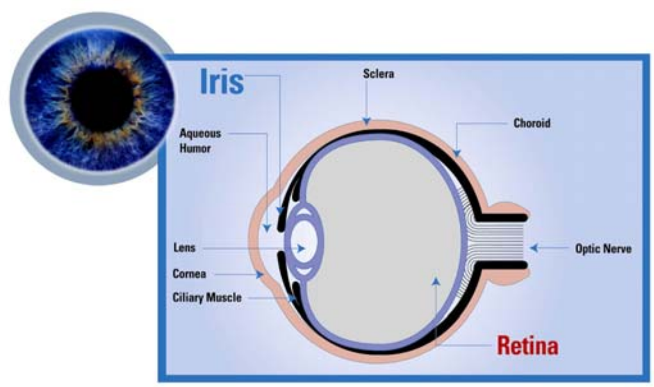

Figure 2: Iris Recognition.[4]

Hand/Finger Geometry

One of the first successful commercial biometric products was a hand geometry system. Typically, a user enters a PIN code to claim an identity, and then places his/her hand on the system,

which takes a picture of the hand. Using mirrors, the picture shows the view of the hand from the top and side. Measurements are then taken on the digits of the hand and compared to those collected at enrollment.

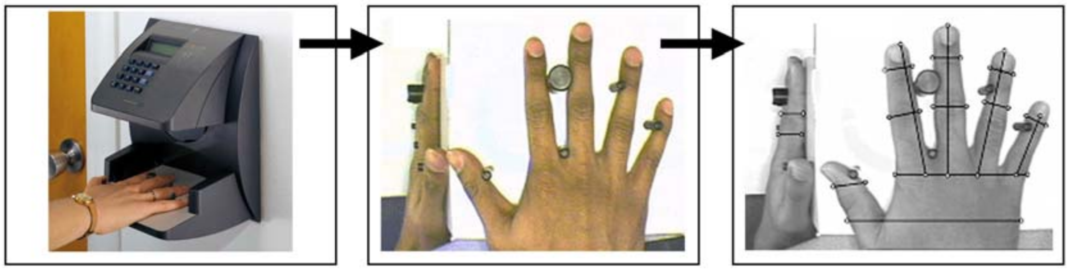

Figure 3: Hand Geometry.[5,6]

Other Biometric Identification Systems

Many other identification methods are in various stages of development and/or commercialization. Following are some examples.

- *Speaker recognition* uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes.
- *Dynamic Signature* measures the speed and pressure one uses when signing his or her name (not what the signature looks like).
- *Keystroke dynamics* measures the typing patterns of an individual.
- *Retina recognition* takes an image of the back of the eye and compares blood vessels with existing data.
- *Gait/Body recognition* measures how someone appears as he or she walks. As in face recognition, this technique is one that humans intuitively use to recognize someone.[7]
- *Facial Thermography* measures how heat dissipates off the face of an individual.

Testing and Statistics

The accuracy of a biometric system is determined through a series of tests, beginning with an assessment of matching algorithm accuracy (technology evaluation), then assessing performance in a mock environment (scenario evaluation), followed by live testing on site (operational evaluation) before full operations begin. Each evaluation serves a different purpose and involves different types of analyses.

Biometric terms, such as recognition, verification and identification, are sometimes used randomly. This is not only confusing, but incorrect as each term has a different meaning.

- Recognition is a generic term and does not necessarily imply either verification or identification. All biometric systems perform “recognition” to “again know” a person who has been previously enrolled.[2]
- Verification is a task where the biometric system attempts to confirm an individual’s claimed identity by comparing a submitted sample to one or more previously enrolled templates.
- Identification is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is “closed-set” if the person is known to exist in the database. In “open-set” identification, sometimes referred to as a “watchlist,” the person is not guaranteed to exist in the database. The system must determine if the person is in the database.

Because of these variances, different statistics must be used for each task.

Verification

False Acceptance Rate (FAR)

The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual’s existing biometric. Example: Frank claims to be John and the system verifies the claim.

Verification Rate

The rate at which legitimate end-users are correctly verified.

Open-Set Identification (Watchlist)

False Alarm Rate

The percentage of times an alarm is incorrectly sounded on an individual who is not in the biometric system's database (the system alarms on Frank when Frank is not in the database), or an alarm is sounded but the wrong person is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

Detection and Identification Rate

The rate at which individuals who are in a database cause a system alarm and are properly identified in an open-set identification (watchlist) application.

Closed-set Identification

Identification Rate

The rate at which an individual in a database is correctly identified.

Standards

Standards help users deploy and maintain their systems in an easier manner, while also promoting longevity and enabling interoperability. There are numerous national and international efforts developing standards for:

- technical interfaces
- data interchange formats
- testing and reporting
- societal issues

Conclusion

The NSTC Subcommittee on Biometrics developed this introductory material in order to better communicate both within the government and with other interested parties. Stating facts and discussing related issues in a consistent, understandable manner, will enable smoother integration of privacy-protective biometric solutions. Federal agencies are working to ensure that their outreach activities are consistent with, and occasionally reference, this suite of documents so that the public, press and Congress are able to easily understand their plans and discuss

them productively. The Subcommittee encourages other entities to also use and reference this material.

This document serves as a general introduction to the field of biometrics; other documents describe key items in more detail. These include:

- Biometrics Frequently Asked Questions
- Biometrics Glossary
- Biometrics History
- Biometrics Overview
- Biometrics Standards
- Dynamic Signature
- Face Recognition
- Fingerprint Recognition
- Hand Geometry
- Iris Recognition
- Palm Print Recognition
- Speaker Recognition
- Biometrics Testing and Statistics
- Vascular Pattern Recognition
- The Privacy of Biometrics

These documents are available at: http://www.biometricscatalog.org/NSTCSubcommittee.

Document References

[1] International Biometric Group <http://www.biometricgroup.com>.

[2] John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

[3] Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).

[4] James Wayman et al, Biometric Systems Technology, Design and Performance Evaluation (London: Springer, 2005).

[5] Maltoni, Davide, Maio, Jain, and Prabhakar, Handbook of Fingerprint Recognition (Springer: New York, 2005).

[6] Secugen Biometrics Solutions <http://www.secugen.com/images/faq02.gif>.

[7] Biometrics: Department of Defense, “Biometrics 101”

<http://www.biometrics.dod.mil/bio101/assets/images/bio101/fingerprint_diagram.jpg>.

[8] Manfred Bromba, “Bioidentification: Frequently Asked Questions” <http://www.bromba.com/faq/fpfaqe.htm#Fingerprint-Sensoren>.

[9] Anil K. Jain, Ruud Bolle, and Sharath Pankanti, Personal Identification in a Networked Society (Kluwer Academic Publishing: Massachusetts, 1999).

About the National Science and Technology Council

The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

A primary objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in a broad array of areas spanning virtually all the mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals. The work of the NSTC is organized under four primary committees; Science, Technology, Environment and Natural Resources and Homeland and National Security. Each of these committees oversees a number of sub-committees and interagency working groups focused on different aspects of science and technology and working to coordinate the various agencies across the federal government. Additional information is available at www.ostp.gov/nstc.

About the Subcommittee on Biometrics

The NSTC Subcommittee on Biometrics serves as part of the internal deliberative process of the NSTC. Reporting to and directed by the Committee on Homeland & National Security and the Committee on Technology, the Subcommittee:

- Develops and implements multi-agency investment strategies that advance biometric sciences to meet public and private needs;
- Coordinates biometrics-related activities that are of interagency importance;
- Facilitates the inclusions of privacy-protecting principles in biometric system design;
- Ensures a consistent message about biometrics and government initiatives when agencies interact with Congress, the press and the public;
- Strengthen international and public sector partnerships to foster the advancement of biometric technologies.

Additional information on the Subcommittee is available at www.biometrics.gov.

Subcommittee on Biometrics

Co-chair: Duane Blackburn (OSTP)

Co-chair: Chris Miles (DOJ)

Co-chair: Brad Wing (DHS)

Executive Secretary: Kim Shepard (FBI Contractor)

Department Leads

Mr. Jon Atkins (DOS)

Dr. Sankar Basu (NSF)

Mr. Duane Blackburn (EOP)

Ms. Zaida Candelario (Treasury)

Dr. Joseph Guzman (DoD)

Dr. Martin Herman (DOC)

Ms. Usha Karne (SSA)

Dr. Michael King (IC)

Mr. Chris Miles (DOJ)

Mr. David Temoshok (GSA)

Mr. Brad Wing (DHS)

Mr. Jim Zok (DOT)

<u>Communications ICP Team</u>

Champion: Kimberly Weissman (DHS US-VISIT)

Members & Support Staff:

Mr. Richard Bailey (NSA Contractor)

Mr. Duane Blackburn (OSTP)

Mr. Jeffrey Dunn (NSA)

Ms. Valerie Lively (DHS S&T)

Mr. John Mayer-Splain (DHS US-VISIT Contractor)

Ms. Susan Sexton (FAA)

Ms. Kim Shepard (FBI Contractor)

Mr. Scott Swann (FBI)

Mr. Brad Wing (DHS US-VISIT)

Mr. David Young (FAA)

Mr. Jim Zok (DOT)

Document Source

This document, and others developed by the NSTC Subcommittee on Biometrics, can be found at www.biometrics.gov.